下载APP

03 | 技术特性：用“铁锁连环”直观理解区块链特点

2021-07-26 赵铭

《说透区块链》 课程介绍 >

讲述：赵铭
时长 11:58 大小 10.98M

你好，我是赵铭。

可能很多人都觉得区块链是一个多么新颖的技术，其实不然。它不过是旧瓶装新酒，本身并没有创造新的技术，只是将几种已经成熟的技术进行组合，是**融合性创新**。

而我们初步开始学习区块链的时候，最重要的就是把握其技术特点，并且了解它的技术基础。今天这一讲，我会通过一个现实中的例子带你探索区块链的技术基础，同时帮助你掌握区块链技术最重要的三个特性。

怎样理解区块链

经常有人问我什么是区块链，一般情况下，我的答案是不一样的。如果你是程序员，我大概率会说区块链是一种分布式 KV 数据库。而如果你是小白，我可能会用几个词回答你：三人成虎，人云亦云，少数服从多数等等。

我的回答不一定准确，但一定最能符合当时受众的心理预期。而当我面对你们，面对拥有各行各业背景的受众时，为区块链概念下一个定义，我的内心是拒绝的。因为每个人理解不同，过于纠结定义反而会忽略本质，所以我们更应该把目光放在理解区块链技术基础和特性上。

其实，区块链技术发展到现在，尤其在以太坊将智能合约的概念与区块链技术融合之后，区块链已经变成了现实与网络的媒介，可以说**区块链是价值的载体，是一种新型的社会生产关系**。

怎么理解这句话呢？我个人的理解是基于区块链技术，我们可以打通现实世界与网络世界的屏障，将物质虚拟化，将价值实体化。未来的互联网流转的不是信息，而是活生生的价值。

未来可期，不过也要始于足下。我们不妨先回归现实世界，前段时间，网上有一张图引起了广泛传播，被网友戏称为“区块链技术实体化”。拿这个例子来说明区块链的技术特性，再适合不过了。

区块链技术实体化

这是辽宁沈阳一小区大门，业主用多把锁串联在一起，形成了一套简单的门禁系统。谁家有车谁就加锁，每把锁都有标识，小区车主只需拿钥匙打开对应锁头，就能打开大门。这样就防止了外来车辆占用小区车位，不得不说，高手在民间。

铁锁连环的具象化

那这个例子是如何具象化表达区块链技术特性的呢？首先，我们需要明确区块链有哪些特性，一般我们认为有 3 点，分别是：

去中心化

可追溯性

不可篡改

结合这个实例，我们来一一理解这几个概念。

去中心化

在这个小区门禁系统中，每把锁代表着一家小区业主，他们不需要物业公司统一管理，只需要管理维护自己的锁就能保证系统的正常运行。

每一把锁有大有小，有贵的有便宜的，业主也可能有多辆车，但在这个系统中他们没有地位上的差别。而且，当有新的业主加入或者有业主搬走，只需要增加或去掉相应的锁就

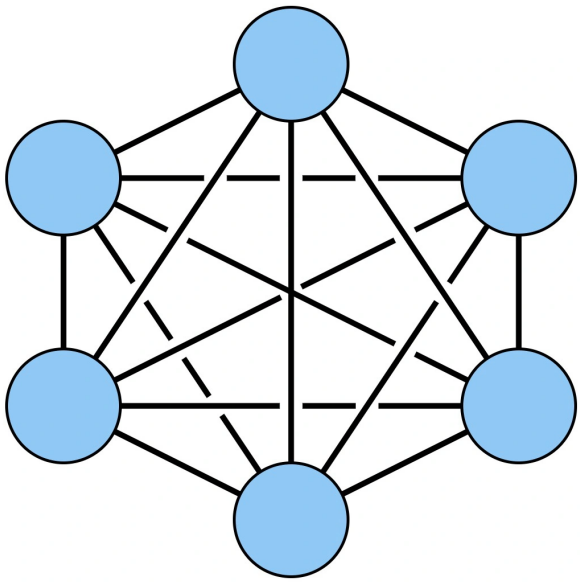
好。

你有没有发现，这里面就蕴含了**去中心化**的概念，门禁不再由物业公司这个“第三方机构”统一管理，每把锁都是管理的一部分。

同样的道理，区块链存在的初衷就是去除中心化的第三方机构（可以回看第 1 讲），整个网络的数据及状态是由网络中所有的节点共同维护的，他们没有地位上的差别，有的只是可支配的资源的不同，且任一节点离线也不会影响系统的运作。

你可以自己试着先推演一下，想要实现去中心化，应该选取怎样的网络模型和存储模型呢？

没有中心节点的系统从某种角度来讲，可以说每一个节点都是中心，每一个节点都能对外提供服务，同样也能从其他节点请求服务，而这也正是点对点网络模型的特性，可以说，节点互为彼此的数据生产者及消费者。

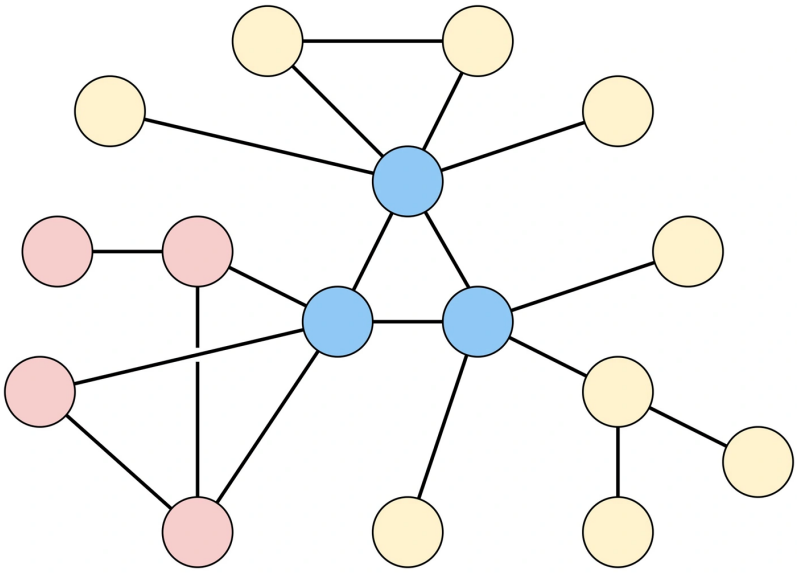


绝对去中心化示意图

另一方面，因为节点角色对等，因此每一个节点存储的数据应该是一致的，都独立地维持一条完整的区块链链式结构，即便一些节点数据丢失，但只要还有一个节点完好，历史数

据就不会丢失。这有效地避免了单点故障带来的系统崩溃，相较于传统的数据灾备模式，其可靠性可以说是万无一失。

当然，去中心化只是一个理想化的状态。现阶段来说区块链去中心化本质上是**相对去中心化**，我们也可以叫做多中心化。我们在理解概念的时候，不仅需要理性思维，更要学会使用感性思维去接受中间过程的渐变。



相对去中心化示意图

可追溯性

在门禁系统中，每把锁记录了业主的相关信息，是跟业主一一绑定的，这就可以在异常情况下对破坏规则的业主进行追责，比如忘记锁门而导致外来车辆进入小区，这体现了该系统的可追溯性。

在实际区块链运转中，同样是完成信息追溯这件事儿，道理虽然相通，但是更为复杂，我来给你说一说。

对单个节点来说，区块链可以被认为是一个**时序数据库**。每一次对系统的操作，实质是在每个节点数据库中存储了相应的数据及日志。且每一份数据都不是离散的存储，而是按时间顺序前后关联在一起，新的数据一定是从某一组之前已存在的数据派生而来。

依照这种关联，如果想回溯数据的状态变更历史是很容易的，只需要依次往前查找，一定会找到数据的初始状态。

而这一切都依赖于区块链存储技术，存储主要关注数据结构以及数据关系，包括交易以及区块的数据结构，交易与区块的关联关系，区块状态的存储模式等等。

不可篡改

另一个技术特点是不可篡改，这是一个比较容易被初学者搞混的概念，**所谓篡改，就是私自的不被认可的修改，而不是不能修改。**

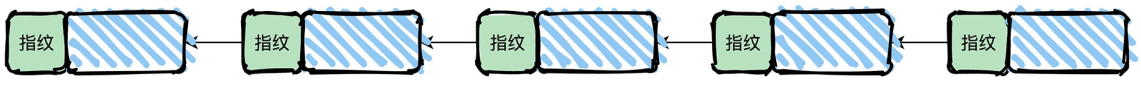
我们回顾例子，可以发现业主手中的钥匙与锁是一一对应的，没有钥匙或者用错误的钥匙，车辆都是进不了小区的。

社会车辆要想进入小区，可能会采取盗用某一业主身份，多配一把钥匙或者添加一把锁，这就是篡改。而只要被业主委员会发现，就会及时纠正错误，将社会车辆清理出去，也就实现了不可篡改。

在区块链中，实现不可篡改需要两种技术来保障。**前面例子里“锁”的功能由密码学技术实现，而“业主委员会”的角色则是由共识算法来扮演。**

前面我们讲过，单个区块链节点中的数据是按时间的先后顺序串联存储的，而串联的关键就利用了密码学中的哈希算法。

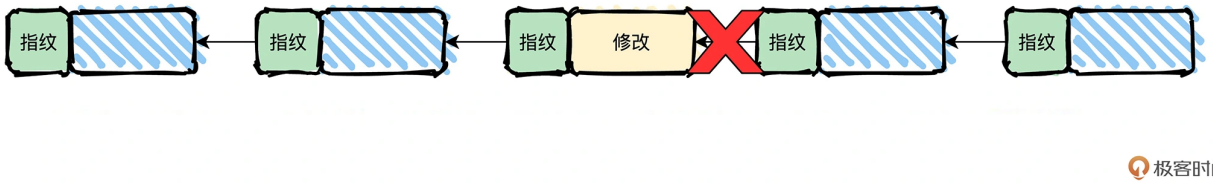
哈希算法可以把一段数据变换成固定长度的数据指纹，而且只要数据有细微变化，得到的指纹也是大不一样的。通过这个方法，我们可以将前一时间段的数据指纹与后一时间段数据整合在一起。周而复始，后一时间段内的数据永远都会包含前一时间段的数据指纹，这样就形成了一条由数据指纹串联的信息链条。



极客时间

数据指纹串联示意图

如果有一个作恶者想要修改中间某一时间段的数据，那么依照哈希算法原理，其对应的数据指纹则会改变。因此他不得不依次修改后续的每一个时间段的数据，否则数据链条就会在他修改的这一刻断掉，不再具备可追溯性。



篡改数据指纹示意图

我们可以把困难进一步放大，想一想如果作恶者真的把本地节点的所有数据都篡改一遍，又要怎么应对呢？

这时候就要让共识算法出马了，它可以保证整个系统的数据不被篡改。所谓共识，就是在一个分布式系统中保持数据的一致性，而如果出现数据不一致，大多数共识算法都遵循少数服从多数的原则。

区块链网络中的每一个节点的数据都是一致的，作恶者只是篡改了自己维护的单个节点，从整个网络的维度来看，依旧是以大多数节点的数据为正确数据。

最后，我想提醒你，看问题不能只看一面，不可篡改其实是一个辩证的特性。少数服从多数的规则意味着如果作恶者能够控制大多数的节点资源，那么篡改区块链是可能的。

在一个健壮且足够分散的网络中，篡改所要付出的成本是巨大的，几乎不可能成功。而一旦成功，剩下的少数派才是妄图破坏区块链共识的作恶者，以太坊的硬分叉（不熟悉可以回看第 1 讲）就是一个典型。

总结

在这一讲中，我们用一个具象化的例子直观理解了区块链的技术特性，同时我们也在其中穿插着带入了区块链技术基础。

如果从纯技术的角度讲，区块链是新一代信息技术的重要推动力，它利用了存储、密码学、点对点网络及共识算法等基础技术的融合，提供去中心化、可追溯以及不可篡改等特性，可以用来解决互联网中的信任及安全问题，从而推动互联网从信息传递向价值传递的变革。

你可能觉得刚才的解读有点书面化，为了帮助你理解，我再给你分享一个通俗版本的：可以说存储是砖头，密码学是钢筋，点对点网络是混凝土，而共识算法是设计图纸，以他们为基础，揉和在一起，就构建了区块链这座精妙的上层建筑。

我想和你强调的是，区块链技术并不是教条主义地照本宣科。比特币是区块链，以太坊也是区块链，技术本身也并没有规定实现的唯一路径。

我更愿意将区块链技术理解为区块链协议，只要能满足其技术特性，人人都可以设计并实现属于自己的区块链。在后面的几讲中，我会着重为你剖析区块链技术基础，希望你知其然，更要知其所以然。

1.区块链是价值的载体，是一种新型的社会生产关系。

2.区块链拥有去中心化、可追溯及不可篡改的技术特性。

3.区块链技术是存储、密码学、点对点网络以及共识算法等基础技术的融合创新。

说透区块链

赵铭 | 区块链服务平台资深架构师

识别二维码
免费试读

讨论

在此之前，你是如何理解区块链的呢，能否用一两句话简短地说明？这一讲以后，你对区块链概念的理解有何变化？

欢迎你在留言区跟我互动，主动思考、积极交流会让你更有收获。

扩展阅读

如果你要进一步了解关于区块链技术的定义，我推荐你阅读Blockchain Technology Defined及What is blockchain technology?这两篇文章，里面有更详细的介绍。

好，我是赵铭，我们下一讲见！

分享给需要的人，Ta订阅后你可得 20 元现金奖励

赞 4 提建议

© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 02 | 着眼今生：揭秘区块链技术的发展现状

下一篇 04 | 存储：区块链的存储设计有定式吗？

更多课程推荐

精选留言 (6)

写留言

周灿新
2021-07-26

学习之前：区块链是一个分布式存储、篡改难度巨大的信息存储技术，目前主要的应用是比特币等数字货币。
学习之后：区块链是一种去中心化、可追溯、不可篡改的信息存储技术，是多种技术结合的融合创新，主要解决的是互联网中的信任和安全问题。

展开

作者回复: 手动点赞

3

闷骚王冠
2021-07-26

老师，区块链领域对普通人有什么经典书籍推荐嘛？

展开

作者回复: 闷骚王冠，你好。如果你懂一点技术，推荐你阅读《区块链革命：比特币底层技术如何改变货币、商业和世界》，如果不太了解技术，可以阅读《区块链：新经济蓝图及导读》

2

大豆
2021-07-26

哈哈，如果有人/机构能够控制多数节点并进行修改。那就真正的颠倒黑白，假的成真的，真的变假的了。

作者回复: 是的，我就想让大家明白这一点。当然，这个困难度还是比较高的，几乎没有可能。

2

高鹏0409
2021-07-29

有个疑问，用户想要合法修改区块链，是怎么做的呢？

展开

作者回复: 合法修改其实就是提交交易，只要交易被认可，被网络接受，交易包含的状态变更就会影响区块链的世界状态

qinsi
2021-07-27

git就是区块链

去中心化：每个用户在本地都有自己的git仓库，并且相互之间可以pull和push
可追溯性：每个git提交都依赖于上一个提交，可以追溯到最初的提交
不可篡改：修改本地的某个历史提交后，其之后的提交的hash值都会变化，导致本地的...
展开

作者回复: 哈哈，是的。这个例子也比较好，但只适合技术人，非技术人就看不懂了

1

1

静静聆听
2021-07-27

我对区块链的理解是，联盟链可以改变生活方式的方方面面，就是20年前的互联网，10年前的移动互联网一样

作者回复: 有这样的趋势，静侯佳音吧

1